18. The storage system having secure data deletion in a multitenant environment of claim **15**, further comprising the one or more processors to:

tag the encrypted data with a tenant tag, wherein the associating the key with the tenant comprises tagging the key with the tenant tag; and

exclude the encrypted data that is tagged with the tenant tag from garbage collection, during an agreed-upon data recoverability time span that starts with the receiving the request from the tenant to delete the data.

19. The storage system having secure data deletion in a multitenant environment of claim **15**, further comprising the one or more processors to:

export the key to the tenant, responsive to the request from the tenant to delete the data;

delete the key as retained in the storage system;

retain the encrypted data in the storage system; and

import the key from the tenant to the storage system, responsive to receiving a request to cancel deletion of the data.

20. The storage system having secure data deletion in a multitenant environment of claim **15**, further comprising the one or more processors to:

export the key to the tenant, responsive to the request from the tenant to delete the data;

retain the key in the storage system, as a master key for approval;

delay deletion of the key during an agreed-upon data recoverability time span that starts with the request from the tenant to delete the data; and

support access by the tenant to the data, using the key that was exported, with approval by the master key, responsive to receiving a request from the tenant within the data recoverability time span to undelete the data, with the tenant returning the exported key to the storage system.

* * * * *